

~~QUESTION~~ ~~ANSWER~~

Cybersecurity
Exam 22/6/2023

- 1) What is a *Known-plaintext attack*?
 An attack scheme to a cryptographic system where the attacker can choose some messages m_1 and, for each m_1 , she can capture the corresponding ciphertext $c_1 = E_{k_1}(m_1)$.
 An attack scheme to a cryptographic system where the attacker can choose some ciphertext message c_1 and, for each c_1 , she can obtain the corresponding element $m_1 = D_{k_1}(c_1)$.

- 2) An attack scheme to a cryptographic system where the attacker can capture some ciphertext messages c_1, c_2, \dots, c_n and, for each c_i , he can obtain the corresponding element m_i .

- DSA is:
 A symmetric block cipher algorithm
 An asymmetric block cipher algorithm
 A hash algorithm
 A signature algorithm

- 3) Given a block cipher E in CBC mode, with block size r and key length n , let (m, c) a pair of plaintext and ciphertext, with message length rr . Which is the complexity of a brute force attack against the secret key, in terms of number of single block encryption operations, supposing that in each attempt the entire message is processed?
 n^2
 trn
 tr^2
 t^2

- 4) What do you need in order to verify the validity of a digital certificate?
 the certificate of the CA that signed the given certificate
 the private key of the CA that signed the given certificate
 your own certificate

- 5) Which is the advantage to use sequence numbers, timestamps, or random values, in an authentication scheme?
 to protect against brute force attack
 to protect against replay or reflection attacks
 to increase the security, in case of password too short
 to distinguish request messages from responses

- 6) Which service is NOT provided by IPsec ESP?
 confidentiality
 delivery confirmation
 data integrity check
 protection against replay attacks

- 7) What is a Spoofing attack?

- listening on the transmission medium along the path between two entities that are communicating forcing a system (the victim) to send the data unencrypted rather than encrypted sending data with a false sender address, impersonating the identity of another system

$m = 1100\ 0000\ 1100\ 0000$

- It is sent encrypted with a symmetric block encryption algorithm $E_k(\cdot)$, with block size equal to 4bit, with key K, using OFB concatenation mode with IV=0001. The complete substitution table of $E_k(\cdot)$ with key K is reported her on the right. The resulting cipher text is:

$c = 1000\ 0010\ 0001\ 1001\ (\text{IV}=0001)$

- Please indicate the value of the modified ciphertext c' and IV' such as the corresponding cleartext (when decrypted with the same key K) will be:

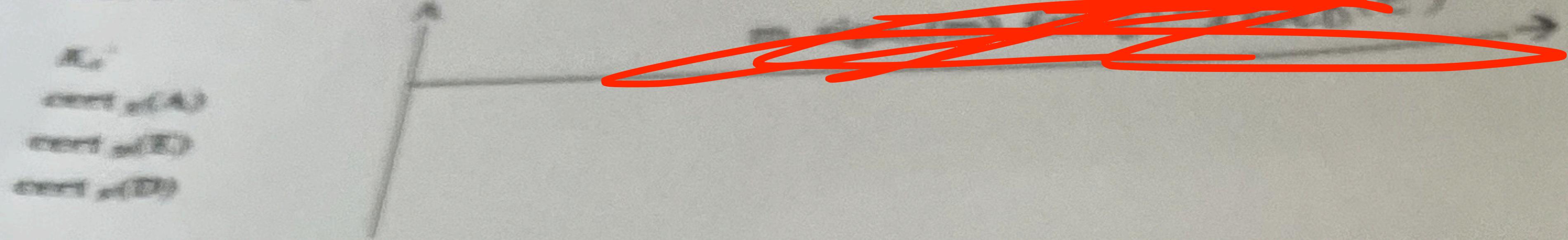
$m' = 1100\ 0000\ 1001\ 0000$

Response:

$c =$

plaintext	ciphertext
0000	1110
0001	0100
0010	1101
0011	0000
0100	0001
0101	0101
0110	0111
0111	1000
1000	1001
1001	1010
1010	1011
1011	1100
1100	1101
1101	1110
1110	1111

- 13) An entity A wants to send a message m to B signed with her private key K_A' . Consider that A has her own private key K_A , the cert $c(B)$, cert $c(D)$, and the cert $c(C)$, while B has cert $c(B)$, cert $c(D)$, cert $c(C)$. Which information should A add to message m in order to let B verifying the signature?



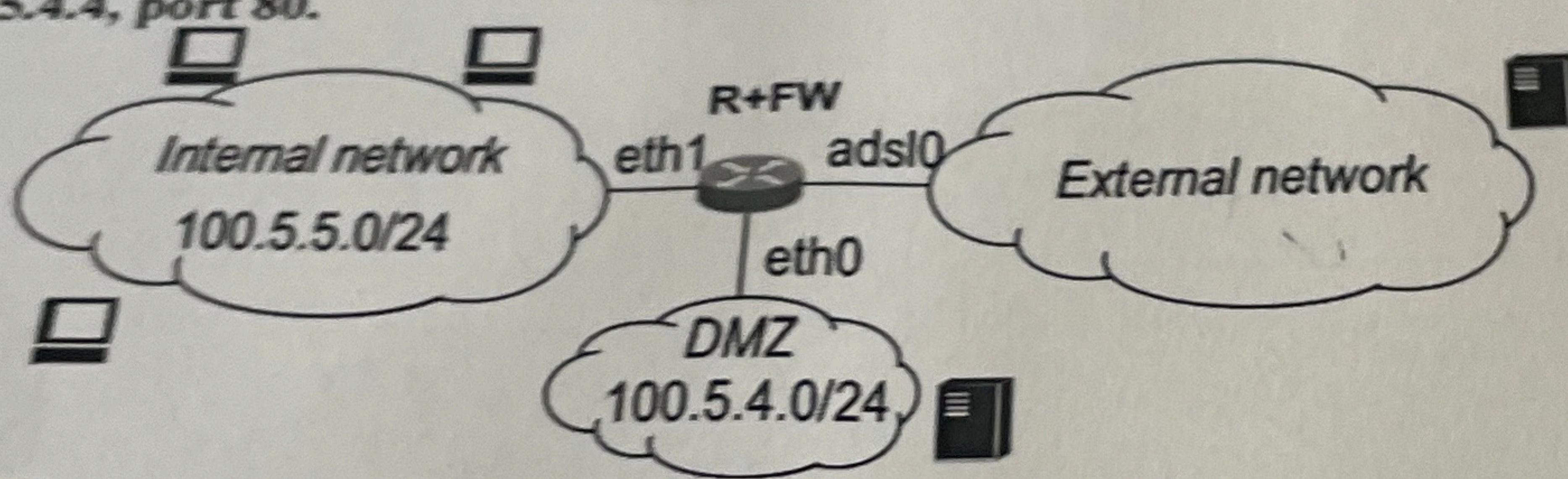
K_A'
cert c(B)
cert c(D)
cert c(C)

- 14) The entity A wants to anonymize a message m to be sent to D, by using the cascade of high-latency anonymizing Mix nodes B and C, in such a way that $A \rightarrow B \rightarrow C \rightarrow D$ is the sequence of nodes that will be involved in the delivery. Assume that K_i' and K_i are the public and private keys of node i (with $i=A,B,C,D$). What is a possible message that A will send to B for such a purpose?

~~X-LKB~~


- 15) Let us consider the following network topology. You are requested to configure the packet filtering router (FW) so that:

- it is possible to communicate in HTTP from any client of the internal network to any server of the external network, limited to server port 80;
- it is allowed any communication between any node of the internal network and DMZ;
- it is possible to establish client/server communications from any node (client) of the external network to the HTTP server 100.5.4.4, port 80.



FORWARD

matching					action	
src_addr	dest_addr	proto	src_port	dest_port	conn_state (NEW / ESTABLISHED)	ACCEPT/DROP



13) An entity A wants to add to message m the digital signature KA^* and $cert_{v(A)}$ and $cert_{v(E)}$ and $cert_{v(D)}$

14) The entity A wants to send a message m to B. Mix no certificate. Assume that A will

15) Let A and B be two entities

pt hm
eth
ads